PC MAGAZINE

SAVE 82% The newest computer GAME DEMOS on CD! COMPUTER GAMING WORLD PLUS CD-ROM Get a new CD every month when you sign up for America's leading computer game magazine!

Windows Your Way

ARTICLE DATE: 09.07.04

By David A. Karp

One thing that makes Windows such an effective platform is its great flexibility: Nearly everything that (on the surface) seems to be hard-coded can be tweaked, turned off, or reconfigured. To that end, Windows XP has the Group Policy Editor (GPE), a tool that lets you not only tinker with the OS but also lock down many of its vulnerabilities.

The GPE has been around since Windows 95, but because it's a power tool, Microsoft has always chosen to hide it (much like the Registry Editor). This is understandable, as there is some potential to wreak havoc, but the GPE's point-and-click design makes it much safer than changing the same settings in Regedit.

RELATED LINKS

Learn all about Win XP SP2 and Longhorn

Note that the Group Policy Editor is not available in XP Home.

The nickel tour. To open the GPE, go to Start | Run and type in gpedit.msc. Those familiar with the Registry Editor or Windows Explorer will feel at home here. There's an expandable tree on the left from which categories are selected and a details list that shows the settings in the selected category on the right.

Branching off the root are two main categories: Computer Configuration and User Configuration. Each branch consists of similar subcategories. Settings in the User Configuration branch affect only the current user (you), while those in the Computer Configuration branch affect all users, plus instances where there is no user, such as the log-on box (or Welcome screen). If similar settings in both areas conflict, the one in the Computer Configuration branch takes precedence.

The categorization of the settings in the GPE can seem haphazard, so you may want to spend a few minutes digging around. The setting names are usually accompanied by a lengthy description, so most settings should be self-explanatory. To change a setting, double-click on it and choose the option you want in the box that appears.

Here are ten of the more useful settings to get you started with the GPE.

1. Dress up Internet Explorer. You can change the look of the IE window, either customizing it to suit your taste or undoing customizations made by your ISP or system manufacturer. Go to User Configuration | Windows settings | Internet Explorer Maintenance | Browser User Interface.

Double-click on the Custom Logo setting to replace the little globe button on the toolbar with your own image (or uncheck the boxes to revert to IE defaults). Double-click on the Browser Toolbar Customizations setting to specify any BMP image file as background wallpaper for your IE toolbar. You can also open the URLs folder (right below the Browser User Interface) to tinker with IE's Favorites and Links menus, or change the URLs used for the search bar and the Online Support menu item (in Help).

2. Start-up and shutdown scripts. You can have Windows run a script whenever the computer is powered on and another just before it shuts down. For instance, write a start-up script to copy the latest version of some document off a server and a shutdown script to copy it back to the server. Or have all the computers in your office run the same script (presumably on a central server) to check for updates, scan for viruses, or do some other task. Go to Computer Configuration | Windows Settings | Scripts (Startup/Shutdown), and double-click on Shutdown. Click on Add to choose a .VBS (VBScript) file on your hard disk.

The corresponding settings in the User Configuration | Windows Settings | Scripts (Logon/Logoff) folder work similarly, except that they're activated every time you log on or off. Settings affecting how all of these scripts work are located in User Configuration | Administrative Templates | System | Scripts and Computer Configuration | Administrative Templates | System | Scripts.

3. Turn off CD/DVD autoplay. The Windows Autoplay feature is responsible for automatically detecting, identifying, and playing CDs and DVDs when you insert them. To disable the feature so that no discs are ever played automatically, go to Computer Configuration | Administrative Templates | System, double-click on the Turn off Autoplay option, and click on Enabled.

4. Disable user tracking. If you hate having Windows record every program you run, every document you open, and every folder path you view, try turning off its User Tracking feature. Go to User Configuration | Administrative Templates | Start Menu and Taskbar and enable the Turn off user tracking feature. This disrupts features that rely on user tracking, such as personalized menus and the My Recent Documents section of the Start menu.

5. Log more security threats. What if you want to keep better track of what others are doing on your computer? By default, the Event Viewer (evenTVwr.msc) tracks application crashes, driver failures, and some security breaches. But you can expand its powers with the Group Policy Editor and its Computer Configuration | Windows Settings | Security Settings | Local Policies | Audit Policy branch. For instance, if you set both the Audit account login attempts and the Audit login attempts settings to Success, the Event Viewer will record failed attempts to log onto your system.

Note that the use of Success and Failure can be a little confusing. Choosing Success for these settings means that you'll log the instances in which your security policy has worked as it should, such as when your computer keeps out an intruder. Conversely, Failure logs those times when security has been compromised on your system.

6. Lock down Internet Explorer. If you've ever set up a computer for the public to use, you know that sooner or later someone will mess it up or try to access something he or she shouldn't. To let the PC act as a "dumb" Internet terminal, with only a Web browser and a mouse, start by disabling context (right-click) menus. Go to User Configuration | Administrative Templates | Windows Components | Internet Explorer | Browser menus, double-click on Disable Context menu, then click on Enabled. There are dozens of similar settings in the neighboring branches to help simplify and secure IE.

7. Clean up the Control Panel. Whether you want to hide sensitive settings from the users of the computers you administer or you just want to reduce clutter on your own system, you can use the Group Policy Editor to remove unwanted icons from the Windows Control Panel. Go to User Configuration | Administrative Templates | Control Panel and double-click on the Show Only Specified Control Panel Applets setting. Click on Enabled, and then click on Show.

If this is your first visit to this box, it will be empty. It's up to you to populate the list with "allowed" applets (CPL files responsible for your Control Panel icons). Click on Add and then type in the filename of each CPL file you wish to allow.

For instance, type in mouse.cpl for the Mouse Properties icon. To see a list of all the CPL files on your computer, open your Windows | System32 folder and sort by type.

8. Configure your Places bar. Choose the folders that appear in the gray Places bar on the left side of most File | Open and File | Save dialog boxes by going to User Configuration | Administrative Templates | Windows Components | Windows Explorer | Common Open File Dialog. Double-click on Items Displayed in Places Bar, click on Enabled, then type in the full pathnames of the folders you wish to appear.

Tip: There is a quick way to specify folder paths without having to type them. Just open Windows Explorer, navigate to the folder you want, and highlight the text in the Address bar (go to View | Toolbars | Address Bar if it's not there). Press Ctrl-C to copy the text, then press Ctrl-V to paste it into the Group Policy Editor.

Note that these settings will not affect Microsoft Office dialogs; you can configure these from within Office. You can also use Creative Element Power Tools to customize both Office and non-Office dialogs.

9. Set stricter password rules. You'll probably want to enforce certain password rules rather than expecting your users to take security seriously on their own. In the Computer Configuration | Windows Settings | Security Settings | Account Policies | Password Policy folder, you can set the minimum password length (in characters) as well as the maximum password age (in days). And if you really want to be a bear about security, turn on the Password must meet complexity requirements option to prevent your users from using their pets' names or birthdays as their passwords.

10. Beef up your firewall. The Security Center is the home of the new firewall built into Windows XP Service Pack 2. Though a substantial improvement over the firewall software in the original XP release, it's still fairly rudimentary. And when you kick in the threat from viruses and spyware, no Windows system is safe right out of the box. Still, you can use the Group Policy Editor to lock some of the back doors Microsoft has left open.

Go to the Computer Configuration | Windows Settings | Security Settings | IP Security Policies on the Local Computer folder, open the Action menu, and select Manage IP filter lists and filter actions. Here, you can filter the network traffic that travels into and out of your computer, based on the IP address of another computer (or even an entire subnet) and the type of data. Click on Add, then follow the instructions in the Filter Wizard to set up a new rule.

Throw away the key. The options you set in the Group Policy Editor are made in the Registry and elsewhere. Once you've locked down your system, you can delete (or just hide) gpedit.msc, thus preventing others from undoing your changes and wreaking havoc on your computer.

David A. Karp is a compulsive tinkerer and the author of Windows XP Annoyances, 2nd Edition, and eBay Hacks (O'Reilly). He can be reached at david@ebayhacks.com .

Copyright (c) 2005 Ziff Davis Media Inc. All Rights Reserved.